WHAT WE CLAIM IS:

1. A method for preventing unauthorized reproduction of first data on a computer having second data provided as Operating System instruction and data, the method comprises the steps of:

generating control data wherein said control data is generated by means of third data which is separate from said second data;

manipulating said second data by inserting said control data within a portion of said second data when installing said first data onto the computer.

2. The method of claim 1 wherein said control data is generated using computer hardware information.

3. The method of claim 1 wherein said control data is generated using data received from a provider of said first data.

4. The method of claim 3 wherein said data received from the provider is non-recurrent.

5. The method of claim 2 wherein said computer hardware information comprises one or more of a component identity, program execution time, program installation time, number of files on a hard disk of said computer, size of hard disk and/or pointer device position.

6. The method according to claim 1, comprising a control sequence further comprising the steps of generating control data and comparing control data to said data stored within said portion of said second data being part of said operating system.

7. A method of preventing unauthorized reproduction of data on a computer having an Operating System, said method comprising the steps of:

providing an instruction set being separate from said operating system;

acquiring hardware-based information using a first control which includes a computer hardware control;

comparing said acquired information with previously stored information;

when said comparison indicates that the hardware information is not changed, acquiring a hardware-based configuration;

generating at least one unique location for a security resource within a portion of said Operating System, based on a hardware identity and/or hardware configuration;

controlling the presence of said resource and, in case the resource is present, performing a self consistency inspection;

in case of a positive inspection result, generating a new unique location;

performing a search for controlling pre-installations in this new unique location and performing a self-consistency; and

in case of self-consistency, processing said data.

8. The method according to claim 7 wherein said computer hardware control comprises acquiring a serial or part number of a machine part.

9. The method according to claim 7 wherein said hardware identifier is used to initialise a random-number generator, which generates one or several random locations within said Operating System file, based on the input information.

10. The method according to claim 9 wherein said locations are always the same as long as the initialising numbers are the same.

11. The method according to claim 7 wherein said resource includes a flag and a correctly stored address of the flags or identity.

12. The method according to claim 7 wherein said self-consistency inspection includes inspection of time of installation of program and/or additional random numbers.

13. The method according to claim 7 wherein the location is unique both with respect to the hardware based information and also the program installation time.

14. The method according to claim 7 wherein in absence of a resource, determining the presence of a first resource and installing the first resource if the determination indicates

the absence of the first resource.

15. The method according to claim 7 wherein if a first resource is present, determining if the method is in an installation mode and if the self consistency exists, if the determination determines a negative, stopping the processing of said data.

16. The method according to claim 7 wherein in case of operation in installation mode, prompting an operator for a code key obtained from a supplier of said set of data.

17. The method according to claim 16 wherein if a correct code key is entered and is consistent, the control is approved and said data is processed.

18. A method for purchasing and securing software in a system comprising a customer computer, a server, a database and a key server, the method comprising the steps of:

purchasing or downloading software by a customer;

installing said software on said customer computer and registering said software;

registering said software having a unique code in said database, using a copy protection system on said customer computer; and

communicating using said installed software with the database for unlocking said software.

19. An article of manufacture comprising: a computer-usable medium having a computer-readable program code and means embodied therein for preventing unauthorized reproduction of first data on a computer having second data provided as Operating System instruction and data and a method for generating control data, wherein said control data is generated by means of third data being separate from said second data, and said second data being manipulated by inserting said control data within a portion of said second data when installing said first data on said computer.

20. A computer data signal embodied in a carrier wave comprising first data, for preventing unauthorized reproduction of first data on a computer having second data provided as Operating System instruction and data and a method for generating control data,

wherein said control data is generated by means of third data being separate from said second data, and said second data is manipulated by inserting said control data within a portion of said second data when installing said first data on said computer.

21. In a computer provided with an operative system, a computer program product for use with an executable computer program, said computer program product comprising: an instruction set for preventing unauthorized reproduction of first data, said computer being provided with second data provided as Operating System instruction and data and the method comprising a step of generating control data, wherein said control data is generated by means of third data being separate from said second data, and said second data is manipulated by inserting said control data within a portion of said second data when installing said first data.

22. A system for managing a security code distribution for preventing unauthorized reproduction of first data, the system being established as a partnership, each partner being one of a plurality of users of said first data, or distributors and/or developers of the same, comprising:

a computer processor means for processing first data;

storage means for storing first data on a storage medium;

first means for initialising the storage medium;

second means for generating an instruction set to be delivered to at least one of said distributors and/or developers for integration with said first data, said instruction set being provided for generating control data for preventing unauthorized reproduction of said first data;

third means for storing said instruction set on said storage medium; and

fourth means for making said instruction set on said storage medium available for distribution to one of said distributors and/or developers on demand.

23. The system according to claim 21 wherein said instruction set is a compiled program code.

24. The system according to claim 21 wherein said instruction set integrated with said first data on a computer is modified with respect to hardware information and requiring

a first code key from said system in return for an identity code.

25. The system according to claim 23 wherein said identity code comprises one or more of hardware identity, installation-based information or a unique identifier.

26. The system according to claim 21 wherein it provides a key of a first type when installing a first set of data, which allows installation of the program.

27. The system according to claim 21 wherein it provides said developer/distributor with a key of second type, which allows producing and/or distributing keys of first type specific for the instruction set of the developer/distributor.

28. A computer unit comprising memory unit, input/output units and a mass storage unit, on which an operating system file is provided for controlling functions of said computer unit, and programs for running application on said computer unit, wherein it further comprises a set of instruction codes for preventing unauthorized reproduction of at least one of said programs running application on said computer unit, through generating control data, and storing said control data within a portion of second data being part of said operating system of said computer, when installing said applications.